(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2005 (15.09.2005)

PCT

(10) International Publication Number
WO 2005/086452 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/EP2005/050895

(22) International Filing Date: 1 March 2005 (01.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0405245.2 9 March 2004 (09.03.2004) GB

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).

(72) Inventors; and

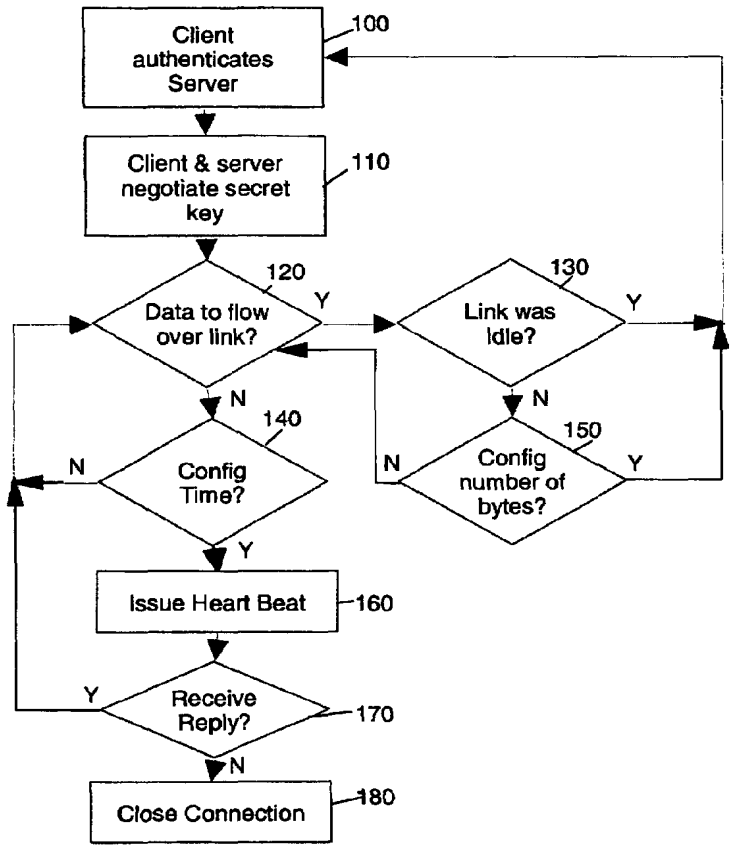
(75) Inventors/Applicants *(for US only)*: **HARRAN, Richard, Michael, Wyn** [GB/GB]; Flat # 3, 2 Wilton Avenue, Southampton Hampshire SO15 2HJ (GB). **HORAN, Michael** [GB/GB]; 12 Olivers Battery Road North, Winchester Hampshire SO22 4JA (GB). **RUMSEY, Jonathan** [GB/GB]; 8 Westgate House, Trafalgar Street, Winchester Hampshire SO23 9DH (GB).

(74) Agent: **WATSON, Justine, Nicola**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester Hampshire SO21 2JN (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,

[Continued on next page]

(54) Title: KEY-BASED ENCRYPTION



(57) Abstract: There is disclosed a method, apparatus, computer program and computer program product for facilitating secure data communications. The secure data communications is carried out using a secret key for encrypting data flowing between first and second entities over a communications link. First it is determined that the communications link has been idle. Once it is determined that there is now data to flow over the previously idle communications link, the generation of a new secret key is initiated. This new secret key is then used for encrypting data sent between the first and the second entities over the communications link.

WO 2005/086452 A1

PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.